Cayley Theorem

Monday, October 20, 2025 9:07 AM

Recall: Permutation Groups

let $\pi = [1\ 4\ 6\ 5\ 2\ 3]$

$= (1) \circ (2\ 4\ 5) \circ (3\ 6)$

$\pi^2 = [1\ 5\ 3\ 2\ 4\ 6]$

Missing:

100 # 1, 2, 7, 8, 9, 13, 14

200 # 4, 7, 17, 27

500 # 2, 3, 5, 6, 8, 11, 18, 19, 20, 24, 25, 26, 27,

9] Notation: for compactness

① use juxtaposition: $(1)(2\ 4\ 5)(3\ 6)$

② omit unit cycle: $(2\ 4\ 5)(3\ 6)$

③ for identity π_0 = $(1)(2)(3)(4)(5)(6)$

use (1) = (1)

10] Prop. if π is written as a product of disjoint cycles, then $ord(\pi)$ = the Least Common Multip of the length of the cycles.

e.g. $\pi = [1\ 4\ 6\ 5\ 2\ 3]$, Find $ord(\pi)$

Soln. $\pi = (2\ 4\ 5)(3\ 6)$

$|C_1| = 3$

$|C_2| = 2$

$\therefore ord(\pi) = lcm(3, 2) = 6$

Thus $\pi^2 = [1\ 5\ 3\ 2\ 4\ 6]$

$\pi^3 = [1\ 2\ 6\ 4\ 5\ 3]$

and so on, until $\pi^6 = [1\ 2\ 3\ 4\ 5\ 6]$

12] e.g.

Find a subgroup of S_7

① of order 3

Soln. $|S_7| = 7!$

Take a cycle of length 3, $c_1 = (2\ 3\ 1)$

let $\pi = c_1 = [2\ 3\ 1\ 4\ 5\ 6\ 7]$

$\therefore H_3 = \{\pi, \pi^2, \pi^3\}$

$\pi^2 = [3\ 1\ 2\ 4\ 5\ 6\ 7]$

$\pi^3 = [1\ 2\ 3\ 4\ 5\ 6\ 7]$

② of order 10

Soln. Take 2 cycles of length 5 and 2.

let $c_1 = (2\ 3\ 4\ 5\ 1)$, $c_2 = (7\ 6)$

$\pi = c_1 \circ c_2 = [2\ 3\ 4\ 5\ 1\ 7\ 6]$

then $H_{10} = \{ \pi, \pi^2, \pi^3, \ldots, \pi^{10} \}$

$$\pi^2 = [3\ 4\ 5\ 1\ 2\ 6\ 7]$$
$$\pi^2 = [4\ 5\ 1\ 2\ 3\ 7\ 6]$$
$$\pi^4 = [5\ 1\ 2\ 3\ 4\ 6\ 7]$$
$$\pi^5 = [1\ 2\ 3\ 4\ 5\ 7\ 6]$$
$$\vdots \qquad\qquad \vdots$$
$$\pi^{10} = [1\ 2\ 3\ 4\ 5\ 6\ 7]$$

13] Thm (Cayley Theorem)

Every group is isomorphic to some subgroup of a permutation group.

14] e.g.

$\mathbb{Z}_2 \cong S_2 = \{ [1\ 2], [2\ 1] \}$; $\theta(0) = [1\ 2], \theta(1) = [2\ 1]$

$\mathbb{Z}_3 \cong \{ [2\ 3\ 1], [3\ 1\ 2], [1\ 2\ 3] \}$

$\mathbb{Z}_5^* \cong ?$

ord (2) = 4 $\qquad\qquad \pi = [2\ 3\ 4\ 1]$

$\theta(1) = \pi_0 = [1\ 2\ 3\ 4]$
$\theta(2) = \pi = [2\ 3\ 4\ 1]$
$\theta(4) = \pi^2 = [3\ 4\ 1\ 2]$
$\theta(3) = \pi^3 = [4\ 1\ 2\ 3]$

$\therefore \quad \mathbb{Z}_5^* \cong \{[1\ 2\ 3\ 4], [2\ 3\ 4\ 1], [3\ 4\ 1\ 2], [4\ 1\ 2\ 3]\}$

End of LNGT

Review :

HW 3, Q2

$$x \in \mathbb{Z}_{15}$$

$$x^{61} \equiv 7 \pmod{15}$$

Soln:

$$\phi(15) = 2 \cdot 4 = 8$$

$$x^{61} \equiv x^5 \equiv 7$$

$$\Rightarrow (x^5)^5 = 7^5$$

$$x^1 = 7^5 \equiv (7^2)^2 \cdot 7$$

15
30
45
60